4000-01-U

DEPARTMENT OF EDUCATION

[Docket ID ED-2021-OCIO-0026]

Privacy Act of 1974; System of Records

AGENCY: Office of the Chief Information Officer, U.S. Department of Education.

ACTION: Notice of a New System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, as amended (Privacy Act), the U.S. Department of Education (Department) publishes this notice of a new system of records entitled "Education Enterprise Identity, Credential, and Access Management (ED ICAM) System" (18-04-05). The ED ICAM System contains identifying information about individual Department employees and contractors.

DATES: Submit your comments on this new system of records notice on or before [INSERT 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. This new system of records will become effective upon publication in the *Federal Register* on [INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER], unless the new system of records notice needs to be changed as a result of public comment. The routine uses listed in the paragraph entitled ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES will become effective on [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER], unless the new system of records notice needs to be changed as a result of public comment. The

Department will publish any significant changes to the system of records or routine uses resulting from public comment.

ADDRESSES: Submit your comments through the Federal eRulemaking Portal or via postal mail, commercial delivery, or hand delivery. We will not accept comments submitted by fax or by email or those submitted after the comment period. To ensure that we do not receive duplicate copies, please submit your comments only once. In addition, please include the Docket ID at the top of your comments.

- Federal eRulemaking Portal: Go to www.regulations.gov to submit your comments electronically. Information on using Regulations.gov, including instructions for accessing agency documents, submitting comments, and viewing the docket, is available on the site under the "Help" tab.

- Postal Mail, Commercial Delivery, or Hand Delivery: If you mail or deliver your comments about this new system of records notice, address them to: Roman Kulbashny, Branch Chief, Security Engineering and Architecture, Information Assurance Services, Office of the Chief Information Officer, U.S. Department of Education, 550 12th Street, SW, Washington, D.C. 20202.

Privacy Note: The Department's policy is to make all comments received from members of the public available for public viewing in their entirety on the Federal eRulemaking Portal at www.regulations.gov. Therefore, commenters

should be careful to include in their comments only information that they wish to make publicly available.

Assistance to Individuals with Disabilities in Reviewing the Rulemaking Record: On request, we will supply an appropriate accommodation or auxiliary aid to an individual with a disability who needs assistance to review the comments or other documents in the public rulemaking record for this notice. If you want to schedule an appointment for this type of accommodation or auxiliary aid, please contact the person listed under FOR FURTHER INFORMATION CONTACT.

FOR FURTHER INFORMATION CONTACT: Roman Kulbashny, Branch Chief, Security Engineering and Architecture, Information Assurance Services, Office of the Chief Information Officer, U.S. Department of Education,550 12th Street, SW, Washington, D.C. 20202. Telephone: (202)245-6848.
If you use a telecommunications device for the deaf (TDD) or a text telephone (TTY), you may call the Federal Relay Service at 1-800-877-8339.

SUPPLEMENTARY INFORMATION:

The records maintained in this system establish a central and authoritative identity management data repository for the Department's enterprise identities. The system of records is maintained to provide authorized individuals access to, or to interact with, the Department's information technology resources. The system will be utilized to support identity management data

activities including, but limited to: (1) the management and governance of digital identity lifecycle activities; (2) the full auditing of all digital identities; and, (3) the management of application and system access.

Accessible Format:

On request to the program contact person listed under FOR FURTHER INFORMATION CONTACT, individuals with disabilities can obtain this document and a copy of the application package in an accessible format. The Department will provide the requestor with an accessible format that may include Rich Text Format (RTF) or text format (txt), a thumb drive, an MP3 file, braille, large print, audiotape, or compact disc, or other accessible format.

Electronic Access to This Document:

The official version of this document is the document published in the *Federal Register*. You may access the official edition of the *Federal Register* and the Code of Federal Regulations at www.govinfo.gov.

At this site, you can view this document, as well as all other documents of this Department published in the *Federal Register*, in text or Portable Document Format (PDF). To use PDF, you must have Adobe Acrobat Reader. You may also access documents of the Department published in the Federal Register by using the article search feature at: www.federalregister.gov. Specifically, through the advanced search feature at this site, you can limit your

search to documents published by the Department.

Jason Gray,
Chief Information Officer.

For the reasons discussed in the preamble, the Office of the Chief Information Officer of the U.S. Department of Education publishes a notice of a new system of records to read as follows:

SYSTEM NAME AND NUMBER:

Education Enterprise Identity, Credential, and Access Management (ED ICAM) System (18-04-05).

SECURITY CLASSIFICATION:

Controlled Unclassified.

SYSTEM LOCATION:

Office of the Chief Information Officer, Information Assurance, U.S. Department of Education, 550 12th Street, SW, Washington, D.C. 20202.

Oracle Corporation, 1501 4th Avenue, Suite #1800/Century Square Building, Seattle, WA 98101 (provides the infrastructure on which the ED ICAM System runs).

IBM SmartCloud for Government, 6300 Diagonal HWY, B001, 1st floor, Boulder, CO 80301-3292 (provides the infrastructure on which the ED ICAM System runs).

SYSTEM MANAGER(S):

Branch Chief, Office of the Chief Information Officer, U.S. Department of Education, 550 12th Street, SW, Washington, DC 20202.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Federal Information Security Modernization Act of 2014, 44 U.S.C. 3551 et seq.; Homeland Security Presidential Directive 12: Policy for a Common

Identification Standard for Federal Employees and Contractors (Aug. 2015); Federal Information Processing Standards (FIPS) 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors (Aug. 2013); Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource (July 2016); OMB Memorandum 10-28, Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (July 6, 2010); OMB Memorandum 14-03, Enhancing the Security of Federal Information and Information Systems (Nov. 18, 2013); and OMB Memorandum 19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management (May 21, 2019).

PURPOSE(S) OF THE SYSTEM:

The records maintained in this system establish a central and authoritative identity management data repository for the Department's enterprise identities. The system of records is maintained to provide authorized individuals with access to, or to interact with, the Department's information technology resources. The system will be utilized to support identity management data activities including, but not limited to:

(1) the management and governance of digital identity lifecycle activities;

(2) the full auditing of all digital identities; and,

(3) the management of application and system access.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

This system contains records on Department employees and contractors who apply for, and were granted access to, the Department's information technology resources.

CATEGORIES OF RECORDS IN THE SYSTEM:

This system of records contains records for employees and contractors related to digital identity, credential, access management, and identity governance including, but not limited to: name; unique numerical/alphanumerical identification numbers; work address; date of birth (DOB); country of citizenship; credential information; contact information; organizational data; identity investigation and summary adjudication information; verification of training requirements or other prerequisite requirements for access to Department information technology resources; and system access data such as account data, roles, privileges, and entitlements.

RECORD SOURCE CATEGORIES:

Information in this system is obtained from official Department information technology systems and is fed into the system of records from the following source systems: the Department's system of records entitled "Investigatory Material Compiled for Personnel Security, Suitability, Positive Identification Verification and Access Control for the Department of Education Security Tracking and Reporting System (EDSTAR)," (18-05-17), which was last published in full in the *Federal Register* at 72 FR 66158 (Nov. 27, 2007);

and the General Services Administration's system of records entitled "HSPD-12 USAccess," (GSA/GOVT-7), which was last published in full in the *Federal Register* at 80 FR 64416 (Oct. 23, 2015).

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

The Department may disclose individually identifiable information contained in a record in this system of records under the routine uses listed in this system of records without the consent of the individual if the disclosure is compatible with the purpose(s) for which the record was collected. The Department may make these disclosures on a case-by-case basis or, if the Department has complied with the computer matching requirements of the Privacy Act of 1974, as amended (Privacy Act), under a computer matching agreement.

(1) *Congressional Member Disclosure.* The Department may disclose information to a member of Congress and to his or her staff from the records of an individual in response to an inquiry from the member made at the written request of that individual. The member's right to the information is no greater than the right of the individual who requested the inquiry.

(2) *Litigation and Alternative Dispute Resolution (ADR) Disclosure.*

(a) *Introduction.* In the event that one of the parties listed in sub-paragraphs (i) through (v) is

involved in judicial or administrative litigation or ADR, or has an interest in judicial or administrative litigation or ADR, the Department may disclose certain records to the parties described in paragraphs (b), (c), and (d) of this routine use under the conditions specified in those paragraphs:

(i) The Department or any of its components;

(ii) Any Department employee in his or her official capacity;

(iii) Any Department employee in his or her individual capacity if the U.S. Department of Justice (DOJ) agrees to or has been requested to provide or arrange for representation for the employee;

(iv) Any Department employee in his or her individual capacity where the Department has agreed to represent the employee; or

(v) The United States where the Department determines that the litigation is likely to affect the Department or any of its components.

(b) *Disclosure to the DOJ.* If the Department determines that disclosure of certain records to the DOJ is relevant and necessary to judicial or administrative litigation or ADR, the Department may disclose those records as a routine use to DOJ.

(c) *Adjudicative Disclosure.* If the Department determines that disclosure of certain records to an adjudicative body before which the Department is authorized

to appear, to a person or entity designated by the Department or otherwise empowered to resolve or mediate disputes, is relevant and necessary to judicial or administrative litigation or ADR, the Department may disclose those records as a routine use to the adjudicative body, person, or entity.

(d) *Disclosure to Parties, Counsel, Representatives, or Witnesses*. If the Department determines that disclosure of certain records is relevant and necessary to judicial or administrative litigation or ADR, the Department may disclose those records as a routine use to the party, counsel, representative, or witness.

(3) *Enforcement Disclosure*. If information in this system of records, alone or in connection with other information, indicates a violation or potential violation of any applicable statutory, regulatory, or legally binding requirement, the Department may disclose records to an entity charged with investigating or prosecuting such violation or potential violation.

(4) *Employment, Benefit, and Contracting Disclosure*.

(a) *For Decisions by the Department*. The Department may disclose a record to a Federal, State, or local agency maintaining civil, criminal, or other relevant enforcement or other pertinent records, or to another public authority or professional organization, if necessary to obtain information relevant to a Department decision concerning the hiring or retention of an employee or other personnel

action, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit.

(b) *For Decisions by Other Public Agencies and Professional Organizations.* The Department may disclose a record to a Federal, State, local, or foreign agency or other public authority or professional organization, in connection with its decision concerning the hiring or retention of an employee or other personnel action, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit, to the extent that the record is relevant and necessary to the receiving entity's decision on the matter.

(5) *Employee Grievance, Complaint, or Conduct Disclosure.* If a record is relevant and necessary to an employee grievance, complaint, or disciplinary action involving a present or former employee of the Department, the Department may disclose a record in this system of records in the course of investigation, fact-finding, or adjudication, to any party to the grievance, complaint, or action; to the party's counsel or representative; to a witness; or to a designated fact-finder, mediator, or other person designated to resolve issues or decide the matter.

(6) *Labor Organization Disclosure.* The Department may disclose records from this system of records to an arbitrator to resolve disputes under a negotiated grievance

procedure or to officials of labor organizations recognized under 5 U.S.C. chapter 71 when relevant and necessary to their duties of exclusive representation.

(7) *Freedom of Information Act (FOIA) or Privacy Act Advice Disclosure*. The Department may disclose records to DOJ or OMB if the Department concludes that disclosure is desirable or necessary in determining whether particular records are required to be disclosed under FOIA or the Privacy Act.

(8) *Contract Disclosure*. If the Department contracts with an entity for the purposes of performing any function that requires disclosure of records in this system to the employees of the contractor, the Department may disclose the records to those employees. As part of such a contract, the Department shall require the contractor to agree to establish and maintain safeguards to protect the security and confidentiality of the disclosed records.

(9) *Research Disclosure*. The Department may disclose records to a researcher if an appropriate official of the Department determines that the individual or organization to which the disclosure would be made is qualified to carry out specific research related to functions or purposes of this system of records. The official may disclose records from this system of records to that researcher solely for the purpose of carrying out that research related to the functions or purposes of this system of records. The researcher shall be required to agree to establish and

maintain safeguards to protect the security and confidentiality of the disclosed records.

(10) *Disclosure in the Course of Responding to a Breach of Data.* The Department may disclose records from this system to appropriate agencies, entities, and persons when (a) the Department suspects or has confirmed that there has been a breach of the system of records; (b) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the Department (including its information systems, programs, and operations), the Federal Government, or national security; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

(11) *Disclosure in Assisting another Agency in Responding to a Breach of Data.* The Department may disclose records from this system to another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (a) responding to a suspected or confirmed breach or (b) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal

Government, or national security, resulting from a suspected or confirmed breach.

(12) *Disclosure in the Course of Responding to a Security Incident*. The Department may disclose records to appropriate governmental agencies, entities, and persons when (a) the Department suspects or has confirmed that there has been a security incident involving the system of records; (b) the Department has determined that as a result of the suspected or confirmed security incident, there is a risk of harm to individuals, the Department (including its information systems, programs, and operations), the Federal Government, or national security; and (c) the disclosure made to such governmental agencies, entities, and persons is necessary to assist in connection with the Department's efforts to respond to such suspected or confirmed security incident or to prevent, minimize, or remedy such harm.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records are stored on an encrypted server within a secured and controlled environment. There are no hardcopy records that require additional storage.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records are retrieved by a combination of name and other unique personal identifiers.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are retained and disposed of in accordance with General Records Schedule (GRS) 3.2, Item 030 (DAA-GRS-

2013-0006-0003) and Item 031 (DAA-GRS-2013-0006-0004). GRS 3.2, Item 030, requires destruction of records when business use ceases; and, GRS 3.2, Item 031, requires destruction of records 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

All physical access to the Department site, and the sites of Department contractors where this system of records is maintained, is controlled and monitored by security personnel who check each individual entering the building for his or her employee or visitor badge. The computer systems employed by the Department offer a high degree of resistance to tampering and circumvention. These security systems limit data access to Department and contract staff on a "need to know" basis and control individual users' ability to access and alter records within the system. All users of this system of records are given a unique user ID with personal identifiers. All interactions by individual users with the system are recorded.

RECORD ACCESS PROCEDURES:

If you wish to gain access to a record regarding you in this system of records, contact the system manager at the address listed above. You must provide the system manager with the necessary particulars such as your full, legal name, date of birth, work address, country of

citizenship, and any other identifying information requested by the Department while processing the request in order to distinguish between individuals with the same name. Requesters must also reasonably specify the record contents sought. Your request must meet the requirements of the regulations at 34 CFR 5b.5, including proof of identity.

CONTESTING RECORD PROCEDURES:

If you wish to contest the content of a record regarding you in this system of records, contact the system manager at the address listed above. You must provide your full, legal name, and any other identifying information requested by the Department while processing the request in order to distinguish between individuals with the same name. You must also specify the information to be contested. Your request must meet the requirements of the regulations at 34 CFR 5b.7.

NOTIFICATION PROCEDURES:

If you wish to determine whether a record exists regarding you in this system of records, contact the system manager at the address listed above. You must provide necessary particulars such as your full, legal name, date of birth, work address, country of citizenship, and any other identifying information requested by the Department while processing the request to distinguish between individuals with the same name. Your request must meet the

requirements of the regulations at 34 CFR 5b.5, including proof of identity.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

None.

[FR Doc. 2021-14409
Filed: 7/6/2021 8:45 am;
Publication Date:
7/7/2021]